United Nations A/69/723

General Assembly

Distr.: General
13 January 2015

Original: English

Sixty-ninth session
Agenda item 91
Developments in the field of information and telecommunications in the context of international security

Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General

Recent years have witnessed considerable progress in the development and application of new information and communication technologies, which potentially could be used for purposes that are inconsistent with the objectives of maintaining international stability and security. An international consensus is now emerging on the need to strengthen international cooperation and formulate relevant international norms, in order to address common challenges in the sphere of information security. To that end, China, Russia, Tajikistan and Uzbekistan jointly submitted an international code of conduct for information security to the General Assembly in 2011 at its sixty-sixth session, which was subsequently co-sponsored by Kyrgyzstan and Kazakhstan. The code of conduct gave rise to extensive international attention and discussion after it was distributed as a document of the General Assembly (A/66/359). Consequently, we revised the code of conduct, taking into full consideration the comments and suggestions from all parties. We now have the honour to enclose herewith the Chinese, Russian and English versions of the revised code of conduct (see annex). With this, we hope to push forward the international debate on international norms on information security, and help forge an early consensus on this issue

15-00392 (E) 260115

Please recycle

It would be highly appreciated if you could circulate the present letter and its annex as a document of the sixty-ninth session of the General Assembly under item 91 of the agenda.

(*Signed*) **Liu** Jieyi
Permanent Representative of the People's Republic of China
to the United Nations

(*Signed*) Kairat **Abdrakhmanov**
Permanent Representative of the Republic of Kazakhstan
to the United Nations

(*Signed*) Talaibek **Kydyrov**
Permanent Representative of the Kyrgyz Republic
to the United Nations

(*Signed*) Vitaly **Churkin**
Permanent Representative of the Russian Federation
to the United Nations

(*Signed*) Mahmadamin **Mahmadaminov**
Permanent Representative of the Republic of Tajikistan
to the United Nations

(*Signed*) Muzaffarbek **Madrakhimov**
Permanent Representative of the Republic of Uzbekistan
to the United Nations

Annex to the letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General

[Original: Chinese and Russian]

International code of conduct for information security

The General Assembly,

Recalling its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Recalling also its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009, 65/41 of 8 December 2010, 66/24 of 2 December 2011, 67/27 of 3 December 2012 and 68/243 of 27 December 2013, on developments in the field of information and telecommunications in the context of international security,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Recognizing the need to prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security,

Underlining the need for enhanced coordination and cooperation among States in combating the criminal misuse of information technologies and, in that context, stressing the role that can be played by the United Nations and other international and regional organizations,

Highlighting the importance of the security, continuity and stability of the Internet and the need to protect the Internet and other information and communication technology networks from threats and vulnerabilities, and reaffirming the need for a common understanding of the issues of Internet security and for further cooperation at the national and international levels,

Reaffirming that policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international Internet-related public policy issues,

Bearing in mind the assessments and recommendations contained in the report of the Group of Governmental Experts established in 2012 on the basis of equitable geographical distribution, in fulfilment of resolution 66/24, and which, in accordance with its mandate, considered existing and potential threats in the sphere of information security and possible cooperative measures to address them,

including norms, rules or principles of responsible behaviour of States and confidence-building measures in the information space, and conducted a study on relevant international concepts aimed at strengthening the security of global information and telecommunications systems,

Stressing the need to develop a common understanding of how norms derived from existing international law relevant to the use of information and communication technologies by States, a measure essential to reduce risks to international peace, security and stability, will apply to State behaviour and the use of information and communication technologies by States, in accordance with paragraph 16 of the report of the Group of Governmental Experts (A/68/98 of 24 June 2013),

Noting that, given the unique attributes of information and communication technologies, additional norms could be developed over time, in accordance with paragraph 16 of the report of the Group of Governmental Experts,

Recognizing that confidence and security in the use of information and communications technologies are among the main pillars of the information society and that a robust global culture of cybersecurity needs to be encouraged, promoted, developed and vigorously implemented, pursuant to General Assembly resolution 64/211, entitled "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures",

Stressing the need for enhanced efforts to close the digital divide by facilitating the transfer of information technology and capacity-building to developing countries in the areas of cybersecurity best practices and training, pursuant to that General Assembly resolution,

Adopts the following international code of conduct for information security:

1. Purpose and scope

The purpose of the present code of conduct is to identify the rights and responsibilities of States in the information space, promote constructive and responsible behaviour on their part and enhance their cooperation in addressing common threats and challenges in the information space, in order to establish an information environment that is peaceful, secure, open and founded on cooperation, and to ensure that the use of information and communications technologies and information and communications networks facilitates the compre' nsive economic and social development and well-being of peoples, and does not ... counter to the objective of ensuring international peace and security.

Adherence to the code is voluntary and open to all States.

2. Code of conduct

Each State voluntarily subscribing to this Code of Conduct pledges:

(1) To comply with the Charter of the United Nations and universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries;

(2) Not to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security;

(3) Not to use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability;

(4) To cooperate in combating criminal and terrorist activities that use information and communications technologies and information and communications networks, and in curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds;

(5) To endeavour to ensure the supply chain security of information and communications technology goods and services, in order to prevent other States from exploiting their dominant position in information and communications technologies, including dominance in resources, critical infrastructures, core technologies, information and communications technology goods and services and information and communications networks to undermine States' right to independent control of information and communications technology goods and services, or to threaten their political, economic and social security;

(6) To reaffirm the rights and responsibilities of all States, in accordance with the relevant norms and rules, regarding legal protection of their information space and critical information infrastructure against damage resulting from threats, interference, attack and sabotage;

(7) To recognize that the rights of an individual in the offline environment must also be protected in the online environment; to fully respect rights and freedoms in the information space, including the right and freedom to seek, receive and impart information, taking into account the fact that the International Covenant on Civil and Political Rights (article 19) attaches to that right special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) for respect of the rights or reputations of others;

(b) for the protection of national security or of public order (ordre public), or of public health or morals;

(8) All States must play the same role in, and carry equal responsibility for, international governance of the Internet, its security, continuity and stability of operation, and its development in a way which promotes the establishment of multilateral, transparent and democratic international Internet governance mechanisms which ensure an equitable distribution of resources, facilitate access for all and ensure the stable and secure functioning of the Internet;

(9) All States must cooperate fully with other interested parties in encouraging a deeper understanding by all elements in society, including the private sector and civil-society institutions, of their responsibility to ensure information security, by means including the creation of a culture of information security and the provision of support for efforts to protect critical information infrastructure;

(10) To develop confidence-building measures aimed at increasing predictability and reducing the likelihood of misunderstanding and the risk of conflict. Such measures will include, inter alia, voluntary exchange of information regarding national strategies and organizational structures for ensuring a State's information security, the publication of white papers and exchanges of best practice, wherever practical and advisable;

(11) To assist developing countries in their efforts to enhance capacity-building on information security and to close the digital divide;

(12) To bolster bilateral, regional and international cooperation, promote a prominent role for the United Nations in areas such as encouraging the development of international legal norms for information security, peaceful settlement of international disputes, qualitative improvements in international cooperation in the field of information security; and to enhance coordination among relevant international organizations;

(13) To settle any dispute resulting from the application of this code of conduct through peaceful means, and to refrain from the threat or use of force.